# Request for Proposal and Quote

# Development of
# Sentinel Routine Querying Tool
# Web Application

Department of Population Medicine

Harvard Medical School and Harvard Pilgrim Health Care Institute

Landmark Center

401 Park Drive

Suite 401

Boston, MA 02215

May 9, 2018

# Table of Contents

# Background

Sentinel is sponsored by the U.S. Food and Drug Administration (FDA) to monitor the safety of FDA-regulated medical products. Sentinel is one component of the Sentinel Initiative, a multi-faceted effort by the FDA to develop a national electronic system that complements previously existing methods of safety surveillance. The Sentinel Coordinating Center resides within the Department of Population Medicine (DPM) at the Harvard Pilgrim Health Care Institute (HPHCI), and is funded by the FDA through the Department of Health and Human Services (HHS) Contract number HHSF223201400030I. Sentinel Collaborators include Data and Academic Partners that provide access to health care data and ongoing scientific, technical, methodological, and organizational expertise.

The purpose of this Request for Proposal (RFP) is to solicit proposals and quotes from candidate organizations to provide design, development, and potential ongoing maintenance as needed for the Sentinel Routine Querying Tool Graphical User Interface (GUI) web application. The application is needed to allow users to interact with a GUI to "design" their own postmarket pharmaceutical surveillance studies, which can then be translated into arguments that will be used in existing SAS-based analytic tools that are part of the existing Sentinel infrastructure.

All content and communications are confidential.

# Proposal Guidelines

This RFP represents the requirements for an open and competitive bidding process. Proposals will be accepted until 6/20/18 at 3pm EST. Any proposals received after this date and time will not be considered. All proposals must be signed by an official agent or representative of the company submitting the proposal.

If the organization submitting a proposal must outsource or contract any work to meet the requirements contained herein, this must be clearly stated in the proposal. Any proposals which call for outsourcing or contracting work must include a name and description of the organizations being contracted. Additionally, proposals must be all-inclusive to cover any outsourced or contracted work.

Contract terms and conditions will be negotiated upon selection of the winning bidder for this RFP. All contractual terms and conditions will be subject to review by HPHCI and will include scope, budget, schedule, and other necessary items pertaining to the project.

## Proposal Contents

Bidders should provide details of their qualifications for this activity based off the current version of functional specifications provided later in this document. The proposal should contain the following information (please use the table in Appendix A for budget and time estimates):

- A presentation or document outlining proposed application and user interface design
    - Artistic renderings of user interface design concepts encouraged
- Examples of existing products that are from a similar industry and/or display skilled, intuitive GUI design
- Details on which programming languages will be used for development
- Details on previous experience with developing tools that required secure transfer of data and user management

- Experience with government contracts preferred, as well as familiarity with Federal Acquisition Regulations (FAR)
- Experience with healthcare analytics preferred
- Previous customer referral(s)
    - Three references with an overview of the tool that was built and the customer's contact information
- Estimated timeline for design and development
- Estimated budget by role and hourly rate (Appendix A) for:
    - Cost for design and development
    - Cost for maintenance support for bug fixes, troubleshooting, and potential upgrades
- Anticipated resources/personnel you will assign to this project (total number, role, title, experience)
- Project management methodologies to be used during development

### Evaluation Criteria

Proposals with that provide the above specified information will be evaluated on the following criteria:

- Overall proposal suitability: Proposal must meet the scope and needs described herein and be presented in a clear and organized manner.
- Organizational experience: Bidders will be evaluated on their experience as it pertains to the scope of this project.
- Previous work: Bidders will be evaluated on examples of their work.
- Cost and timeline: Bidders will be evaluated on the cost of their solution(s) based on the work to be performed in accordance with the scope of this project as well as how long it will take to design and develop the application.
- Technical expertise and experience: Bidders will be evaluated on documented staff technical expertise and experience.

Please submit all communications through info@sentinelsystem.org.

If you intend to submit a proposal, please email by **5/28/18, before 3pm EST**.

If you have any questions, please email them by 6/1/18. SOC will host a Q/A session via webinar on 6/12/18 to answer those questions, as well as any follow-up questions. Details about the session will be provided upon request.

Terms for Sentinel/HPHCI contracts can be found in Appendix B.

## Project Purpose and Description

The Sentinel Initiative is a FDA funded project to conduct postmarket surveillance of pharmaceuticals in the United States. Sentinel Operations Center (SOC) relies on a distributed network of healthcare data contributors with data in a Common Data Model (CDM) format to routinely execute analytic programs on behalf of FDA to answer pharmacoepidemiologic inquiries.

SOC developed a network infrastructure and methodology for querying the distributed network through a framework of standardized SAS-based analytic programs that can be configured repeatedly by users, distributed, executed, and subsequently return data for further analysis in a short timeframe. These tools are leveraged at a high frequency to conduct investigations for FDA to assess drug safety. Because

of the desire to increase accessibility, usability, and understanding of analytic programs, SOC is exploring the development of a web application with an intuitive Graphical User Interface (GUI) to increase use of existing tools.

Based on current known requirements, SOC determined the need for a web-based application that allows users to construct and submit a valid "query" (list of arguments) for an analytic program using a web interface. The web application should allow authenticated users to create, view, edit, and "submit" (store) these lists of arguments. The web application should also allow authorized remote applications that are part of SOC's internal infrastructure to retrieve these lists of arguments. The web application design should be flexible, automatically updating its user interface as new versions of the program are released by SOC.

The desired web application must provide an intuitive user interface. SOC requests that developers place a heavy emphasis on user experience (UX) and graphical elements, over a text driven experience. The goal is to allow users to feel as if they have "designed" their own query by populating a series of parameters that are assembled in a logical and intuitive user interface. The web application should also be flexible, allowing SOC to adjust the elements of the GUI without developer intervention. It also must be designed to allow for increasingly complex argument submissions in the future. The result of a user's transaction with web application should be that the values entered in the GUI are accessible via REST API in JSON format. SOC applications will ultimately access and use that data to create the SAS-based queries distributed to the collaborating healthcare providers. This tool does not need functionality to create the SAS-based queries.

# Project Scope (Functional Specifications)

## Terms and Definitions

1. **Web Application:** used to refer to both the user-accessible "front-end" as well as the "back-end" web service of the tool to be developed
2. **Program:** the purpose of the web application is to allow the user to specify arguments for SAS analytical programs. The analytical programs will be referred to as a "Program," below. Arguments specified by the user in the GUI will populate the parameters of a Program.
3. **Parameter:** a variable for which a value may be assigned that will be passed as input to an execution of a Program.
4. **Parameter Set:** a collection of parameters that define all possible inputs to a version of a Program. A "Parameter Set" is represented by a markup file that will be included in a Program's source code repository (the "Parameter Set Source Application"). One or more Parameter Sets may be present for a version of a Program. A "Parameter Set" defines not only the valid parameters for the Program version, but also additional information related to GUI controls, how the GUI controls should be rendered in the web application user interface, references to help/documentation information, and argument validation.
5. **Argument:** a user-selected value or values for a Parameter.
6. **Argument Set ("Query"):** a list of valid arguments created by a user for all required and relevant optional parameters for a version of the Program. These submissions will be stored in the web application's database and will be accessible to other web applications via the web application's REST API (see "Edit/View Argument Sets User Interface" and "Web Application API," below).

Once retrieved from the web application, the user's Argument Set will be used as input for a Program.

7. **User Administration Interface:** a web page that will allow administrator users (defined as users with the administrator access group) to create and modify user accounts
8. **View Argument Sets User Interface ("Query Library"):** a user-accessible front-end web page that will allow the user to view all draft or submitted Argument Sets they (or another member of their access group(s)) have created.
9. **Edit/View Argument Sets User Interface ("Query Builder"):** a user-accessible front-end web page that will allow the user to edit an existing draft Argument Set save a draft Argument Set, or submit a draft Argument Set.
10. **Deployment Package:** the deliverable for this project is a deployment package, which contains the web application, all utility and library dependencies required to instantiate the web application as a service, guidelines and documentation for initial configuration of the application and its dependencies, links to download locations(s) for any external dependencies that are not provided as part of the deployment package, and appropriate documentation of all controls and configuration options provided to administrator users.

## User Interface Requirements

This section defines all user interfaces and user interface capabilities that the web application must provide.

1. **User Login Interface**
    a. The web application must provide a login interface that requests a username and password from users who attempt to access service resources.
        i. This interface should be bypassed if the user is already authenticated (has an authentication cookie).
    b. The web application must redirect requests for access to secure application user resources (i.e., webpages) to the user login interface if the user is not authenticated.
    c. The web application must provide appropriate descriptive error information to the user if user authentication fails. If external authentication is not specified in the application configuration file:
        i. The user login interface should authenticate user login requests against the list of authorized users present in the web application's database
            1. The web application must store users' username, encrypted password, and list of user access groups (as defined in the User Administration interface) in the web application's database.
            2. If authentication succeeds, the user should be issued a browser cookie that contains a unique token used for the purposes of authentication with the web application.
        ii. The user login interface should allow users to request a password reset link, and must provide a password reset interface that allows a user who accesses the link to reset the password to their account.

1. The web application must use the SMTP mail server specified in the application configuration file to send an e-mail to the address associated with the user for whom the password reset request was issued that contains a password reset link.
2. The password reset interface must allow the accessing user to enter a new password that matches the password complexity requirement defined in the application configuration file.
3. The web application must use the SMTP mail server specified in the application configuration file to send an e-mail to the address associated with the user for whom the password reset request was issued that contains a notification that the user's password was reset.

iii. If a user successfully logs into the application using a system-generated temporary password, the user should be redirected to the password reset interface defined above, and must be required to change their password.

d. If external authentication is specified in the application config file:

i. The web application must redirect user login requests to the Atlassian Crowd platform defined in the application configuration file, redirecting the user back to the web application upon successful login.

1. The web application must respect the Atlassian Crowd SSO cookie for the purposes of authentication, authenticating this cookie with the Atlassian Crowd application when the user requests access to a secure resource.

The login interface must redirect password reset requests to the Atlassian Crowd platform "Reset Password" interface.

**2. User Administration Interface**

a. The web application must provide a User Administration interface that allows users with the "administrator" access group to create users and modify user details.

b. The User Administration Interface should only be accessible if external authentication is not specified in the application configuration file.

c. The User Administration Interface must be accessible from the View Argument Sets User Interface via a button or link. The button/link should only appear to users in the "administrator" group, and only if external authentication is not specified in the application configuration file.

d. The User Administration Interface must allow users with the "administrator group" to modify the name, e-mail, and access groups of users.

e. The User Administration Interface must allow users with the "administrator" group to create new access groups by entering a name and description for the group.

f. The User Administration Interface must allow users with the "administrator" group to create a new password for a user without entering the user's existing password.

g. The User Administration Interface must allow users with the "administrator" group to create a new user account, entering a name, e-mail, and access groups for the user.

i. The web application must generate a temporary password for any user account created using this interface.

**ii.** If specified in the application configuration file, the web application must use the SMTP server specified in the application configuration file to send an e-mail to the address associated with the new user that contains the user's username, temporary password, initial connection information and any other details specified in the application configuration file.

**3. View Argument Sets User Interface ("Query Library")**

a. The web application must provide a user interface that allows the user to access a list of Argument Sets that the user is authorized to view.

b. This interface must allow the user to create a new Argument Set by interacting with a graphical element (button or link).

i. Administrators should have the ability to disable this feature for specific user groups.

c. The View Argument Set User Interface must allow the user to create a copy of an existing Argument Set, preserving all selected Arguments and user access groups.

i. Administrators should have the ability to disable this feature for specific user groups.

ii. The interface must allow the user to re-enter or modify metadata for the copied Argument Set.

1. The interface must prompt the user to enter a new Argument Set ID if the specified ID is already associated with an existing Argument Set.

d. The View Argument Sets User Interface must allow the user to access the Edit/View Argument Set User Interface for a new or existing Argument Set.

e. The View Argument Sets User Interface must indicate when each Argument Set was created, last modified, and submitted.

i. The View Argument Sets User Interface may also display standard metadata elements common to all Argument Sets as specified in the application configuration file (e.g. Name, Description, Program Name, Program Version, Parameter Set Name, Creator, etc.).

f. The View Argument Sets User Interface must allow the user to search all Argument Sets that they can access (**based on their access group membership**).

i. The View Argument Sets User Interface must provide the ability to filter Argument Sets by standard metadata elements and/or by text string (i.e., "any Argument value containing the text entered").

**4. Edit/View Argument Set User Interface ("Query Builder")**

a. The web application must provide a user interface that allows the user to define argument values for a new or existing (draft) Argument Set.

i. If an existing Argument Set is opened in the Edit/View Argument Set User Interface, and the Argument Set is already opened for editing by another user, the Edit/View Argument Set User Interface should default to a read-only view (i.e. modifications cannot be entered or saved). The user should be presented with a notification that indicates why modifications may not be saved in this view.

    1. If a "Simultaneous Edit" Read-Only timeout threshold is specified in the application configuration file, when an existing Argument Set is opened in the Edit/View Argument Set User Interface, and the Argument Set is not locked, the user should be presented with a timer that indicates the amount of time they have to edit the Argument Set.

        a. The timer should include a descriptive message that indicates either a) for the user that is able to edit the Argument Set, that the timer represents the amount of time remaining to edit the Argument Set, and that the Argument Set will be saved upon timeout, and b) for all other users, that the timer represents the amount of time remaining until the Argument Set is editable.

        b. The timer should start counting down from the defined "Simultaneous Edit" Read-Only timeout threshold specified in the application configuration file.

        c. While the timer is running, the Edit/View Argument Sets Interface should default to a read-only view for all other users, and should display the timer and timer message.

        d. When the timer expires, the web application should save the information entered in the Argument Set, return the user to the View Argument Sets user interface, and present the user with a descriptive notification that the timer has expired and the Argument Set has been saved automatically.

        e. The Edit/View Argument Set User Interface must be accessible both via the View Argument Set User Interface and via hyperlink (specifying a base URL and an "ID" query parameter).

    2. The web application must allow existing Argument Sets to be accessed by direct hyperlink to the Edit/View Argument Set User Interface, if a valid ID query parameter is provided and an Argument Set with the given ID exists.

        a. If the requesting user is not already authenticated (does not have an authentication cookie), the user should be redirected to the user login page, and should be directed back to the specified Argument Set upon successful login.

        b. If the user does not have appropriate access groups to view the Argument Set, as defined either in the application's database or in the external authentication application, the user should be presented with a descriptive error message.

c. If the hyperlink contains a **valid** "id" query parameter, the Argument Set with the matching "id" should be loaded and displayed to the user.

ii. The web application must allow new Argument Sets to be created by direct hyperlink to the Edit/View Argument Set User Interface, if a valid ID query parameter is provided and an Argument Set with the given ID does not exist.

a. If the requesting user is not already authenticated (does not have an authentication cookie), the user should be redirected to the user login page, and should be directed back to the specified Argument Set upon successful login.

b. If an Argument Set does not exist with the valid "id" specified in the query parameters, the web application must create a new Argument Set.

c. The web application must save al query parameters provided to the application database when the Argument Set is saved.

b. The Edit/View Argument Set User Interface must allow the user to specify the Program, Program Version, and Program "Type" with which a new Argument Set will be associated.

i. A Default Program may be specified in the application configuration file.

ii. A default Program Version, or "latest" version may be specified in the application configuration file.

c. The Edit/View Argument Set User Interface must, upon user selection of a Program and Program version, if more than one Parameter Set is available for the selected Program version, allow the user to specify which Parameter Set they wish to use for the current Argument Set.

d. The Edit/View Argument Set User Interface must display a series of graphical elements to the user. These elements are defined in the Parameter Set associated with the Program and Program version when a Program, Program version, and Parameter Set version are selected.

i. The Edit/View Argument Set User Interface must load all parameter information that will be used to render the parameter-specific GUI controls from the Parameter Set selected by the user (or from the default Parameter Set, if only one Parameter Set is available for the selected Program and Program version).

1. E.g., parameter name, user-friendly description and entry guidance, GUI control type (e.g., drop-down menu, date picker, free-text entry, code list entry), allowable values, value source (external application REST API sources), validation regular expression, cross-parameter validation, tooltips, documentation links, etc.

e. The Edit/View Argument Set User Interface must allow for logically grouped parameters in the user interface in accordance with the structure of the Parameter Set (e.g., if multiple parameters are grouped together, this grouping should be visually reflected in the user interface).

f. If specified in the Parameter Set, the Edit/View Argument Set User Interface must allow a user to add additional instances of a parameter or grouping of parameters (also referred to as "Scenarios"), up to a maximum number of entries for a given parameter or grouping of parameters as specified in the Parameter Set.

    i. If specified in the Parameter Set, the Edit/View Argument Set User Interface may allow the user to "add" additional instances of a parameter grouping to the Argument Set and user interface, up to a specified maximum number of instances of a parameter group that may be present at one time (specified in the Parameter Set).

g. If specified in the Parameter Set, the Edit/View Argument Set User Interface must allow a user to copy and paste a list of Arguments for a given Parameter.

    i. The import functionality must support plaintext and comma-separated values.

h. If specified in the Parameter Set, the Edit/View Argument Set User Interface must allow a user to upload/import a list of Arguments for a given Parameter.

    i. The import functionality must support plaintext (.txt) and comma-separated value (.csv) files.

    ii. The import functionality should allow the user to upload multiple files of the same type (multiple files of varying types should be rejected upon submission).

    iii. The import functionality should convert files uploaded this way into the appropriate database value(s) and store them in the application database. Once this operation is complete, the files should be deleted.

i. The Edit/View Argument Set User Interface must allow the user to save a draft version of the Argument Set without "submitting" the Argument Set.

j. The Edit/View Argument Set User Interface must allow the user to specify one or more user access groups that can view the Argument Set. These access groups will be used to define which users are able to view the Argument Set in the View Argument Sets User Interface or access an Argument Set directly by hyperlink.

k. The Edit/View Argument Set User Interface must allow the user to specify one or more user access groups that can edit the Argument Set. These access groups will be used to define which users are able to edit an existing draft Argument Set.

l. The Edit/View Argument Set User Interface must allow the user to submit a completed Argument Set.

    i. "Completed" is defined as an Argument Set for which all required parameters, as defined in the Parameter Set, are populated, and for which all selected values are valid in accordance with validation present in the Parameter Set.

    ii. If specified in the Parameter set, the Edit/View Argument Set User Interface must validate user-submitted Arguments for the specified Parameters.

        1. If the specified validation is "cross-parameter" (i.e., the value of one argument depends on the value of another argument), and the related parameter does not pass the validation specified in the Parameter Set, the Edit/View Argument Set must provide a descriptive error message

that indicates the relationship between parameters, and prevents the submission.

2. If the specified validation is for a code construct (e.g. no special characters are allowed) and the submitted values in the argument do not meet that criteria, the Edit/View Argument Set must provide a descriptive error message.

3. If the specified validation requires an external API data reference, the Edit/View Argument Set User Interface must obtain reference data from the external application specified in the Parameter Set and must perform the validation type specified (contains, matches, etc.). Connection information for the external application API should be stored in the application configuration file.

iii. If a user attempts to submit an Argument Set that does not pass validation, the Edit/View Argument Set User Interface must present the user with an error prompt that indicates which element(s) of their submission did not pass validation. If additional validation error message information is present in the selected Parameter Set for the parameter(s) that did not pass validation, this information should be shown to the user.

iv. The Edit/View Argument Set User Interface must prompt the user to confirm their submission.

m. The web application must send one or more outbound web requests to each remote application, endpoint specified in the application configuration file, when an Argument Set is completed.

This functionality will allow the web service to integrate with arbitrary remote applications that can receive web requests, to trigger remote operations in real-time when an argument submission is completed.

i. The web application should send a POST request to each remote application endpoint specified in the application configuration file, using the credentials specified for each application. The POST request should contain no information other than the name of the originating web service and the ID of the Argument Set that was made.

ii. If the POST request fails, the failure should be written to the web application logs, including destination address and reason for failure.

iii. If the POST request succeeds, the success information should be written to the web application logs, including destination address and response (if one is provided by the remote application).

n. The Edit/View Argument Set Interface must display/output a graphical rendering of the selected Arguments after the Argument Set has been saved, if the Arguments required to generate this graphical rendering have been entered.

i. The graphical rendering should utilize image resources defined in the Parameter Set.

ii. The graphical rendering is intended to show an illustration of a study design for sharing with a 3rd party without access to the web application.

## System Requirements

The following sections indicate all non-user-interface features and capabilities required.

1. **Web Application API**
    a. The web application must provide a REST API interface that allows service users, authenticated per-request using BASIC authentication over TLS 1.2, to:
        **i. Obtain a list of all Argument Sets:**

        **Returns:**
        Argument Set ID
        Parameter Set ID (Parameter Set that was populated)
        Program ID

        **ii. Obtain a single Argument Set's content by ID**

        **Providing:**
        Argument Set ID
        **Returns:**
        All Arguments populated in the Argument Set
        Argument Set ID
        Parameter Set ID
        Program ID
        Name, Description, Creator, Date metadata

        **iii. Create an Argument Set with a given name and description (generating an Argument Set ID automatically)**

        **Providing:**
        Name
        Description
        Program ID
        Parameter Set ID
        **Returns:**
        n/a

        **iv. Create an Argument set with a given name, description, and ID**

        **Providing:**
        Name
        Description
        Program ID
        Parameter Set ID
        Argument Set ID
        **Returns:**
        n/a

        **v. Update an Argument Set to set Program ID, Program version, Parameter Set ID, and submission metadata (e.g., name, description)**

vi. **Update an Argument Set that has a selected Parameter Set, assigning argument values for the Argument Set**

2. **Web Application Scheduled/Background Tasks**

   a. The web application must obtain the most up to date Parameter Sets from the Parameter Set source application defined in the application configuration file.

      i. This task should be executed on the interval defined in the application configuration file.

      ii. The web application must store all Parameter Set information retrieved from the Parameter Set source application in the web application's database.

      iii. The web application must retrieve all remote resources specified in each Parameter Set (e.g. images) and store these files in the web application's directory.

3. **Application Configuration File**

   a. The web application must allow users with access to the server to set application configuration options for the web application using a configuration file. Application configuration should be reloaded when the web application service is restarted.

      This functionality allows application administrators to configure application dependencies (e.g. database connection) and integration with external applications (i.e. allowing additional applications to receive web requests from the web application when an Argument Set is submitted).

   b. The web application configuration file should contain the following elements:

      i. Database connection string, configuration information, and database credentials

      ii. The option to enable authentication / SSO using an external Atlassian Crowd service ("external authentication")

         1. Atlassian Crowd service location (base URL) and service account credentials (authentication and authorization)

         2. Atlassian Crowd SSO domain name (if required)

      iii. Password Complexity Requirement Regular Expression

      iv. SMTP Mail Server address and credentials

         1. Default/template contents for Account Creation, Password Reset Link, and Password Reset Acknowledgment e-mails

      v. View Argument Set Interface configuration

         1. Metadata elements visible in the View Argument Set Interface

      vi. Edit Argument Set Interface configuration

         1. "Simultaneous Edit" Read-Only timeout threshold, in minutes

      vii. Integration URIs (Uniform Resource Indicators) and service accounts

         1. The web application configuration file should allow administrators to define the following integration URIs

a. Parameter Set Source Application(s)
    i. Used to obtain Parameter Sets for each specified Program
    ii. Parameter Set Retrieval Interval
        1. Indicates the interval at which to check for new Parameter Sets
b. Parameter Value Source REST API URI(s)
    i. Used to obtain selectable parameter values for the specified parameters if a remote application is specified as a data source in a Parameter Set
c. Argument Set web request target location(s)
    i. Used to trigger remote events when an Argument Set is submitted

4. **User Authentication and Authorization**
    a. The web application must support single-sign-on authentication with the Atlassian Crowd platform as a configurable authentication option.
    b. If an external authentication is not enabled, the web application must authenticate users against an access control list stored in the web application's database.
        i. The initial access control list must contain a default administrator user.
    c. If external authentication is enabled, the web application must be able to obtain a user's access group membership from the Atlassian Crowd platform for the purposes of authorization using Atlassian Crowd REST APIs.
        i. If external authentication/authorization is not enabled, the web application must utilize its own stored access group information to determine user authorization.
    d. The web application must only allow a user to view and access Argument Sets if the user is in one or more access groups associated with the Argument Set(s) in question.
    e. The web application must store an association of application access group names with each Argument Set or submissions and must make authorization decisions based on a user's group membership as obtained from Atlassian Crowd REST APIs.
5. **Service Account Authentication and Authorization**
    a. The web application must store all external application credentials required for enabling integrations in the application database. Sensitive credentials stored in this way (e.g., passwords) must be protected in accordance with security best practices.

## Non-functional Requirements

1. **Technologies and Frameworks**
    a. The web application front-end user interface should ideally be implemented using modern technologies or frameworks (e.g. ReactJS/AngularJS, modern CSS frameworks).

b. The web application back-end web service should ideally be implemented using modern technologies or frameworks (e.g. NodeJS).

Note: The examples provided above are not strict requirements for this application. Priority is given to technologies or frameworks that confer application responsiveness, scalability, and ease of maintenance.

**2. Compatibility**

a. The web application must be compatible with the most recent versions of the most commonly used desktop web browsers (Internet Explorer, Firefox, Chrome).

b. The web application should be compatible with Internet Explorer 10, if possible.

c. The web application should be compatible with the most recent versions of the most commonly used mobile web browsers (Chrome, Safari).

i. The web application UI should automatically adjust/resize when viewed on a mobile device.

**3. Dependencies**

a. The web application deployment package must include all external utility and library dependencies that are required for its instantiation as part of the initial deployment package.

b. The web application deployment package must include reference material that enumerates each library dependency and the required version(s) of each library or dependency.

c. The web application must be able to be operate in a Windows environment and be configured as a Windows service.

i. The web application should ideally also operate in a Linux environment (if possible)

d. The web application must be able to be hosted on a Microsoft Azure Virtual Machine.

e. The web application must support the latest stable version of PostgreSQL for the application's database.

**4. Security**

a. The web application must be able to be configured to utilize SSL for all external HTTP connections (i.e., connections to non-localhost addresses) using the existing Sentinel SSL wildcard certificate. The web application should not support insecure HTTP connections from any external source.

b. The web application must always require authentication for access to all provided resource.

c. The web application must, when setting new user passwords, properly validate that passwords match the complexity requirement defined in the application configuration file.

d. The web application must encrypt user passwords stored in the web application's database using a secure, industry-standard encryption algorithm.

5. **Logging**
    a. The web application must log all application errors to a text file (.log) located in the application installation directory. If the log file does not exist when logging is attempted, a new log file should be created. Log files should contain:
        i. Timestamp of errors / warnings generated by the application
        ii. Descriptive information related to the error for debugging purposes
        iii. Stack trace of the error (if possible)
6. **Scalability**
    a. The web application should support asynchronous execution of tasks
7. **Availability/Recoverability**
    a. The web application should ideally rely on as few external service dependencies for usual operation as possible.
    b. If the web application cannot resolve required service dependencies (e.g., access/identity management platform if in use, web application database), this information should be logged to the application log file.
8. **Documentation**
    a. The web application deployment package must include technical documentation resources that include the following elements:
        i. Guidelines for initial deployment and configuration of a new instance of the web application, including any configuration changes that must be made to application dependencies (if any are required), and the appropriate version(s) of each application dependency (including external service dependencies, such as the web application's database).
        ii. Documentation of all required and optional settings included in the web application configuration file, explanation of the use and impact of each setting, and example values for each setting.
        iii. Documentation of all available in-UI administrator options, selectable values, and their impact.
        iv. Documentation of default administrator credentials, if applicable.
        v. Documentation of the database model / schema (tables, columns, data types, and how they relate to the application).
        vi. REST API Documentation
            1. For each specified endpoint, a description of the endpoint's function, required request type, request parameters, error codes (and their meanings), success code(s), and example requests (with example results)

## Request for Proposal/Quote Timeline

**Request for Proposal Timeline:**

If you intend to submit a proposal, please notify SOC at info@sentinelsystem.org by **5/28/18 before 3pm EST**. Only bidders who have informed SOC of intent to bid will be considered.

All proposals in response to this RFP are due no later than **6/20/18 at 3pm EST**.

Evaluation of proposals will be conducted from 6/21/18 to 7/17/18. If additional information or discussions are needed with any bidders during this window, the bidder(s) will be notified.

The selection decision for the winning proposal will be made no later than **7/17/18 at 3PM EST**.

Notifications to bidders who were not selected will be completed by 7/17/18 at 5pm EST.

Upon notification, contract negotiation with the winning bidder will begin immediately.

## Ownership

This activity is Work for Hire (WFH). All functionality generated by this activity is property of FDA. HPHC owns all intellectual property.

## Contact Information

Please send all emails to info@sentinelsystem.org. Your primary point of contact is the Systems Development team lead, Max Ehrmann.

### Appendix A: Budget Templates

| **Design and Development** | | | | |
|---|---|---|---|---|
| **LABOR:** | | | | |
| Name | Role | Rate | Hours | Cost |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | | | |
| **TOTAL LABOR** | | | 0 | $0.00 |
| | | | | |
| **Other Costs:** | | | | |
| | | | | $0.00 |
| | | | | $0.00 |
| | | | | $0.00 |
| TOTAL Other Costs | | | | $0.00 |
| | | | | |
| **TOTAL DURATION (Weeks)** | | | | |
| **TOTAL COSTS** | | | | $0.00 |

| Maintenance | | | | |
|---|---|---|---|---|
| **LABOR:** | | | | |
| Name | Role | Rate | Hours | Cost |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | $0.00 | 0 | $0.00 |
| | | | | |
| **TOTAL LABOR** | | | 0 | $0.00 |
| | | | | |
| **Other Costs:** | | | | |
| | | | | $0.00 |
| | | | | $0.00 |
| | | | | $0.00 |
| TOTAL Other Costs | | | | $0.00 |
| | | | | |
| **TOTAL DURATION (Weeks)** | | | | |
| **TOTAL COSTS** | | | | $0.00 |

## Appendix B: Sentinel Terms and Conditions

**Federal Acquisition (FAR) Regulations by Reference**

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text.

| | | |
|---|---|---|
| FAR 52.202-1 | Definitions | NOV 2013 |
| FAR 52.203-3 | Gratuities | APR 1984 |
| FAR 52.203-5 | Covenant Against Contingent Fees | APR 1984 |
| FAR 52.203-6 | Restriction on Subcontractor Sales to the Government | SEP 2006 |
| FAR 52.203-7 | Anti-Kickback Procedures | OCT 2010 |
| FAR 52.203-8 | Cancellation, Rescission, and Recovery of Funds for Illegal or Improper Activity | JAN 1997 |
| FAR 52.203-10 | Price or Fee Adjustment for Illegal or Improper Activity | JAN 1997 |
| FAR 52.203-7 | Anti-Kickback Procedures | OCT 2010 |
| FAR 52.203-12 | Limitations on Payments to Influence Certain Federal Transactions | OCT 2010 |
| FAR 52.209-6 | Protecting the Government's Interest When Subcontracting with Contractors Debarred, Suspended, or Proposed for Debarment | AUG 2013 |
| FAR 52.215-2 | Audit and Records – Negotiations Alt. II | OCT 2010 |
| FAR 52.215-17 | Waiver of Facilities Capital Cost of Money | OCT 1997 |

| | | |
|---|---|---|
| FAR 52.215-19 | Notification of Ownership Changes<br>• This clause is only applicable for subcontracts with institutions subject to Subpart 31.2. | OCT 1997 |
| FAR 52.216-7 | Allowable Cost and Payment<br>• If Cooperating Institution is an educational institution, the words "Subpart 31.3" are substituted for "Subpart 31.2" in paragraph (a).<br>• If Cooperating Institution is a nonprofit organization other than an educational institution, the words "Subpart 31.7" are substituted for "Subpart 31.2" in paragraph (a). | JUN 2013 |
| FAR 52.219-8 | Utilization of Small Business Concerns | JUL 2013 |
| FAR 52.219-9 | Small Business Subcontracting Plan Alt. II | OCT 2001 |
| FAR 52.222-3 | Convict Labor | JUN 2003 |
| FAR 52.222-21 | Prohibition of Segregated Facilities | FEB 1999 |
| FAR 52.222-26 | Equal Opportunity | MAR 2007 |
| FAR 52.222-35 | Equal Opportunity for Special Disabled Veterans, Veterans of the Vietnam Era, and Other Eligible Veterans | SEP 2010 |
| FAR 52.222-36 | Affirmative Action for Workers with Disabilities | OCT 2010 |
| FAR 52.222-37 | Employment Reports on Disabled Veterans and Veterans of the Vietnam Era | SEP 2010 |
| FAR 52.223-6 | Drug-Free Workplace | MAY 2001 |
| FAR 52.225-13 | Restrictions on Certain Foreign Purchases | JUN 2008 |
| FAR 52.227-1 | Authorization and Consent Alt. I | DEC 2007 |
| FAR 52.227-2 | Notice and Assistance Regarding Patent and Copyright Infringement | DEC 2007 |
| FAR 52.232-18 | Availability of Funds | APR 1984 |
| FAR 52.249-2 | Termination for Convenience of the Government (Fixed-Price) | APR 2012 |
| FAR 52.249-4 | Termination for Convenience of the Government (Services) (Short Form) | APR 1984 |
| FAR 52.249-5 | Termination for Convenience of the Government (Educational and Other Nonprofit Institutions) | SEPT 1996 |
| FAR 52.249-8 | Default (Fixed-Price Supply and Service) | APR 1984 |
| FAR 52.249-14 | Excusable Delays | APR 1984 |

**Health and Human Services Acquisition (HHSAR) Regulations by Reference**

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text.

| | | |
|---|---|---|
| HHSAR 352.202-1 | Definitions | DEC 2006 |
| HHSAR 352.203-70 | Anti-lobbying | JAN 2006 |
| HHSAR 352.224-70 | Privacy Act | JAN 2006 |
| HHSAR 352.227-70 | Publications and Publicity | JAN 2006 |
| HHSAR 352.231-71 | Pricing of Adjustments | |
| HHSAR 352.233-71 | Litigation and Claims | JAN 2006 |
| HHSAR 352.242-70 | Key Personnel | JAN 2006 |
| HHSAR 352.242-71 | Tobacco-Free Facilities | JAN 2006 |
| HHSAR 352.242-73 | Witholding of Contract Payments | JAN 2006 |
| HHSAR 352.242-74 | Final Decisions on Audit Findings | APR 1984 |

**Additional Requirements and Certifications**

To the extent applicable to the Services provided under the Services Agreement, Offeror hereby certifies and provides assurance that it is in compliance with, will comply with, and agrees to the following:

**1. Restriction on Employment of Unauthorized Alien Workers**

Offeror certifies that none of the funds received from this award will be used to employ workers described in section 274A(h)(3) of the Immigration and Nationality Act. (18 U.S.C. 1324a).

**2. Protection of Human Subjects**

As applicable, Offeror assures that adequate safeguards shall be taken whenever using human subjects in research and an institutional review committee composed of sufficient members with varying backgrounds to assure complete and adequate review of projects involving the use of human subjects has reviewed and approved the projects. Informed consent, where appropriate, shall be obtained by methods consistent with Title 45 Code of Federal Regulations, Part 46, Subpart A, "Protection of Human Subjects," and specifically Section 46.107, "Special Assurances."

**3. Debarment**

Offeror shall comply with Executive Orders 12549 and 12689, "Debarment and Suspension," as implemented by Department of Commerce regulations at 15 CFR part 26. Offeror represents and certifies that Offeror is not, and will not use in the direct performance of this project the services of any person who is debarred, suspended, proposed for debarment, declared ineligible, or voluntarily excluded from participating in any activity contemplated by this Agreement by any Federal department or agency. Offeror will promptly disclose in writing to HPHC if any person who is performing services hereunder is debarred or if an action, suit, claim, investigation or legal or administrative proceeding is pending or, to the best of Offeror's knowledge, threatened relating to the debarment of Offeror or any person performing services hereunder.

**4. Lobbying**

Offeror certifies that, to the best of its knowledge:

(a) No Federal appropriated funds have been paid or will be paid, by or on behalf of the Offeror to

any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the award, continuation, renewal, amendment or modification of any Federal grant, cooperative agreement, contract, or loan. Offeror shall complete and submit the then-current "Certification Regarding Lobbying," available at 45 C.F.R. Part 93 Appendix A, in accordance with its instructions.

(b) If any funds other than Federal appropriated funds have been paid or will be paid as described in subparagraph (a) above, the Offeror shall complete and submit the then-current "Disclosure Form to Report Lobbying," available at 45 C.F.R. Part 93 Appendix B, in accordance with its instructions.

**5. Civil Rights and Equal Employment Opportunity**

Offeror certifies that she is in compliance with E.O. 11246, "Equal Employment Opportunity," as amended by E.O. 11375, "Amending Executive Order 11246 Relating to Equal Employment Opportunity," and as supplemented by regulations at 41 CFR part 60, "Office of Federal Contract Compliance Programs, Equal Employment Opportunity, Department of Labor."

**6. Clean Air Act and Federal Water Pollution Control Act**

In the event that total funding hereunder exceeds $100,000, Offeror shall comply with the Clean Air Act of 1970 (42 U.S.C. 7401 et seq.) and the Federal Water Pollution Control Act (33 U. S. C. 1251 et seq.) as amended. Violations must be reported to the Federal sponsoring agency and the Regional Office of the Environmental Protection Agency.

**7. HIPAA Compliance and Subject Information Confidentiality**

The parties may receive from each other certain health or medical information in the performance of this Service Agreement ("Protected Health Information," or "PHI," as defined in 45 C.F.R. Section 160.103). Use or disclosure of PHI is subject to protection under State and Federal law, including the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191 ("HIPAA") and implementing regulations, Privacy of Individually Identifiable Health Information and Security Standards for the Protection of Electronic Protected Health Information, codified at 45 CFR Parts 160 and 164, subparts A, C, and E. Each party shall comply with such law and implementing regulations as applicable during the term of this Agreement and after termination.

Offeror will comply with all applicable state laws concerning the confidentiality and security of personally identifiable information (e.g., first and last name in combination with social security number or driver's license number, etc.), including but not limited to Mass. Gen. Laws chs. 93H and 93I.

No other provision in this Agreement shall be construed to override the provisions of this Article.